International Conference on Topical Issues in Nuclear Safety,
IAEA, 3 - 6 September 2001, Vienna

Topical Issues Paper No. 1

RISK INFORMED DECISION MAKING

Authors

F. NIEHAUS, IAEA
T. SZIKSZAI, IAEA

Reviewers

L. MORALES, CNAT, Spain
C. SHEPHERD, H.M. Nuclear Installations Inspectorate, United Kingdom
G. TOKMACHEV, Institute Atomenergoproekt, Russian Federation
D. TRUE, Erin Engineering and Research, Inc., United States of America

1. RATIONALE

To date, probabilistic safety assessments (PSAs) have been performed for more than 200 nuclear power plants (NPPs) worldwide and are under various stages of development for most of the remaining NPPs. The state-of-the-art is to have a full scope Level 2 PSA (including external events and low power and shutdown) which is maintained as a 'living PSA' with regular updating. Modern computer technology allows frequent recalculations of the PSA to evaluate the impact of changes in operation or design and allows use of the PSA in the form of safety or risk monitors. There is a general agreement, as documented in various IAEA Safety Standards, that the deterministic approach to nuclear safety should be complemented by a probabilistic approach.

Though PSAs have been used extensively in the past, it was usually limited to a variety of applications on a case by case basis as deemed necessary or useful. There is now a recent development led by the USA, and followed by several other countries, to move to a much expanded use of PSA in what is termed 'risk informed decision making'. The main driving force behind this movement is the expectation that the use of risk insights can result in both improved safety and a reduction in unnecessary regulatory requirements, hence leading to a more efficient use of resources for NPP operators and the regulatory authority.

One of the key challenges in truly risk informed decision making is the reconciliation of PSA results and insights with traditional deterministic analysis. This is particularly true when it comes to defence in depth and safety margins. PSA results often conflict with deterministic insights. If a method of reconciling these conflicts is not defined, then risk informed can become deterministic plus PSA. This results in PSA being an additional layer of requirements rather than a tool for optimized decision making. Alternatively, if PSA information is always used to override deterministic considerations, then that is a "risk based" approach, not risk informed.

This issue is less important if the plant is being upgraded (e.g. risk informed design improvements). However, when optimization of requirements (e.g. relaxation of regulations) is being pursued, it becomes a central issue. Table I demonstrates the complementary nature of deterministic and probabilistic approaches to safety evaluation.

A prerequisite for such an expanded use is the availability of a high quality 'living PSA', which supports the various applications. The PSA quality should be commensurate with its intended application. This means that there is not one standard for judging the adequacy of the PSA but that the quality of the PSA should be judged in relation to each specific use or application. Many efforts have been devoted to achieve consistency and quality of PSAs. They include peer reviews (e.g. the IAEA IPERS/IPSART programme), PSA standardization efforts (e.g. United States Nuclear Regulatory Commission (USNRC) PRA Procedures Guide, IAEA PSA Guidelines, the recent draft American Society of Mechanical Engineers (ASME) PSA Standard, IAEA–OECD/NEA guidance for regulatory review of PSA) and compilation and comparisons of PSAs for similar types of NPPs, including

TABLE I. SUMMARY OF STRENGTHS AND LIMITATIONS OF DETERMINISTIC AND PROBABILISTIC APPROACHES TO SAFETY

	DETERMINISTIC	PROBABILISTIC
STRENGTHS	· Underlying principles of defence in depth, redundancy and diversity provide technically sound design criteria. · Responsible for outstanding safety record. · Resulting requirements expressed in pass/fail rules and are straightforward to implement and to verify compliance. · Safety margins developed for structures, systems and components provide protection for range of accident challenges beyond the design basis.	· Inclusive treatment of any accident scenario that potentially contributes to risk; not confined to design basis accidents. · Accident frequencies and consequences dealt with quantitatively based on realistic assumptions. · Facilitates ranking of technical issues and events based on contribution to risk. · Quantitative approach to evaluating impacts of uncertainties on risk estimates. · Provides consistent way to feedback operating experience to refine risk predictions.
LIMITATIONS	· Limited to somewhat arbitrarily defined design basis accidents and single failure criterion (or N-2 rule); protection for beyond design basis accidents only implicitly provided. · Assessment that decisions create no undue risk to the public made on a qualitative and subjective basis. · Deals with a limited set of uncertainties by use of conservative assumptions and safety margins; many uncertainties not explicitly addressed. Combination of conservative assumptions tends to obscure understanding of realistic behaviour. · Apart from need to demonstrate that such accidents are incredible, provides no explicit assessment of the capabilities to protect against beyond design basis accidents which dominate the public risk.	· Results highly dependent on and limited by state of knowledge; subject to change as knowledge evolves. · Use of conservatism skews results; realistic treatment not always feasible. · Requires robust and complete risk model and identification of all sources of dependency to avoid optimistic results. · Uncertainties in risk estimates may be too large to support certain decisions. · Limited to accidents caused by randomly occurring failures; requires assumed validity of the deterministic basis of the plant. · Human actions treatment very difficult and no viable approach to errors of commission.

comparisons of the success criteria and failure rates used. Another concept being pursued is to provide a quality grading of the major PSA elements and subelements required to support a specific application and to assess the quality of the PSA in these required areas.

This paper draws on some information compiled in IAEA-TECDOC-1200 'Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants' [1]. This document has been drafted as a result of several meetings, and the IAEA would like to gratefully acknowledge the participation of all the experts who contributed to the drafting. Ms A. Gomez Cobo was the responsible officer for that document.

1.1. BACKGROUND

Historically, PSAs have primarily been performed by regulatory bodies who have used them to gain generic risk insights (e.g. WASH-1400 [2] and NUREG 1150 [3]), or by licensees, who have used them for a variety of purposes, including compliance with regulatory requests to support a safety case, identification and understanding of key plant vulnerabilities, and analysis of the impact of proposed design or operational changes. PSAs have also been used to evaluate the design of new plants. Having invested considerable resources in developing PSAs, there is a desire on the part of both licensees and regulators to use the insights derived from them to enhance plant safety, while operating the nuclear stations in the most efficient manner. PSA is an effective tool for this purpose as it assists in targeting resources where the largest benefit to plant safety can be obtained.

An NPP PSA, in principle, has the potential to provide an understanding of the inherent risk of operating the plant over a much wider range of conditions than traditional deterministic methods, which generally define what is assumed to be a bounding set of fault conditions. Furthermore, the adoption of conservative assumptions relating to plant and system performance is an accepted approach to addressing uncertainty when performing these deterministic analyses. By using PSA, which considers a much wider range of faults, takes an integrated look at the plant as a whole (system interdependencies), uses realistic criteria for the performance of the plant and systems and tries to quantify the uncertainties, more 'risk informed' decisions can be made. The PSA, therefore, is useful to improve plant safety and safety management.

However, while the PSA can be seen, in principle, to provide a broader perspective on safety issues than deterministic approaches, the application of sound engineering principles has been demonstrably successful in achieving a high level of safety. Besides, while PSA is a useful tool to improve plant safety, its weaknesses and limitations need also to be acknowledged.

1.2. PSA IN DECISION MAKING

The extent to which PSA results can contribute to a decision is dependent on the level of detail of the PSA model, its quality, its completeness, and on whether the subject of the decision is amenable to analysis using a PSA. For certain specific and limited applications a relatively simple PSA model may be adequate. However, for other applications, such as when a PSA is to be used as a day to day tool for decision making at NPPs, all aspects of the model are brought into play, and a detailed, comprehensive model is necessary. As the understanding of plant performance improves, and the weaknesses, limitations and technical difficulties associated with the PSA are progressively remedied, the quality and usefulness of the PSA will increase.

The extent to which Member States are making use of PSAs in decision making varies greatly. Not all countries have a regulatory framework for the use of the probabilistic approach in place. Most countries use PSAs in the design area to support NPP upgrading, backfitting and plant modifications. Also, for new NPP developments, PSA has become a standard tool in design. Recently, emphasis has been given to the use of PSA in determining the safety classification of systems and components. There is a large potential for use of PSA in the operational safety area, in particular regarding the optimization of technical specifications, configuration control during maintenance and determination of test intervals [4]. However, more extensive use in this area is limited by the quality of the available PSAs in some countries to support such applications.

The opinions of a number of specialists and users have been collected at a recent meeting. They indicate the following broad prioritization in terms of the present usefulness of the application to risk management. Though it is noted that clearly this prioritization could well be different for a specific plant, Table II may nevertheless provide useful indications to those managing resources. In addition to the areas of applications listed, risk informed prioritization of regulatory inspection is recently being explored in several countries.

TABLE II. PRIORITIES FOR PSA APPLICATIONS

Application	**Priority**
Use of PSA to support NPP design	High
Use of PSA to support NPP upgrade and back-fitting	High
Use of PSA to evaluate safety issues	High
Use of PSA to improve operator training programmes	High
PSA based evaluation and rating of operational events	High
Use of PSA to improve emergency operating procedures	Medium
Use of PSA to support accident management	Medium
Risk based configuration control	Medium
Use of PSA to support NPP periodic safety review	Medium[a]
Use of PSA in maintenance	Medium
Use of PSA in connection with Technical Specifications	Medium
Use of PSA to support emergency planning	Low
Risk based safety indicator	Low
Graded QA	Low

[a]Although this application has appeared overall as being of medium priority, it was clear that the usefulness of PSA within the periodic safety review (PSR) process is very much dependent on the degree to which PSA has previously been applied to the NPP in question.

Whatever the level of detail adopted, the model must reflect the current status of the plant. Therefore, if the PSA is to be of continuing use in the enhancement and understanding of plant safety, it must be updated or modified when necessary to reflect changes to the plant and its operating practices, and also to reflect improvements in methods. This has led to the concept of 'living PSA' (LPSA). Thus, a PSA used to support decision making must have a credible and defensible basis, and must reflect the design and operation of the plant. Also, it is very important that the PSA be accepted by the plant and the regulator. Therefore, all those facets of the PSA quality that are independent from the intended applications such as traceability, consistency, documentation, quality assurance, etc., are very important aspects that need to be considered when developing a PSA and afterwards when using it for different applications. Some of the applications can be performed in advance of initiating changes at the plant, some applications require on-line use. Acceptance of the PSA by the plant is enhanced by the significant involvement of plant staff in its development. Acceptance of the PSA by the regulator is enhanced through a clearly defined review process and established procedures for using the results in practice.

One criticism often leveled at PSAs which, for many people, limits their usefulness, is the uncertainty within the PSA community of how to address some of the modelling elements. Typically, such uncertainties are addressed by making particular assumptions or adopting a specific model for an element of the PSA. There are ongoing efforts to improve the accuracy and to standardize or at least harmonize PSA and PSA applications. However, rather than being an impediment to using PSA, this identification of uncertainties can be turned into a strength. An understanding of the impact of these uncertainties on the PSA results, obtained, for example, by performing sensitivity analyses, can lead to more robust decisions. This understanding is dependent on the sources of information used to develop the PSA model and the adequacy with which the information is documented. Therefore, in order to achieve this goal, a comprehensive documentation of the PSA is necessary, including identification and specification of the underlying assumptions. Consideration of weaknesses and limitations must of course also be given in the traditional deterministic studies and is implicit in making conservative assumptions and using safety margins.

2. STATUS OF TOPICAL ISSUE

2.1. ISSUES ON WHICH THERE IS GENERAL AGREEMENT

2.1.1. PSA as a complement of the deterministic approach

All countries operating or constructing nuclear facilities are required to establish legal and governmental mechanisms to ensure nuclear safety, including the establishment of a regulatory body. "Responsibility should be assigned to the regulatory body for authorization, regulatory review and assessment, inspection and enforcement and for establishing safety principles, criteria, regulations and guides" [5]. Historically, this responsibility was implemented using a deterministic approach. Though explicit or implicit probabilistic considerations were included, these were converted to deterministic requirements such as defence-in-depth, single failure criterion, or definition of safety

margins. Many reasons were responsible for this fact: Immature probabilistic methodology, capability limitation of computer hardware and software, limited availability of component failure data and understanding of physical phenomena, limited understanding of human behaviour, etc. Thus, rather than basing the argument on probabilistic considerations, there was more emphasis on requiring redundancy, diversity or safety margins. In addition, probabilistic results are difficult to comprehend, a problem facing PSA even now. Recently, the licensing of nuclear installations is making more extensive and formal use of probabilistic considerations by changing to the use of a deterministic **and** probabilistic approach. Historically, the use of probabilistic considerations has always been more common in, Argentina, Canada, Netherlands, South Africa, UK, the USA, and in some Scandinavian countries.

2.1.1.1. Design safety

Related to design, probabilistic considerations are included in the IAEA international Safety Standards. The General Nuclear Safety Objective is defined in Ref. [6] as: "To protect individuals, society and the environment from harm by establishing and maintaining in nuclear installations effective defense against radiological hazards." This is supplemented by two complementary Safety Objectives related to radiation protection and technical aspects. The Technical Safety Objective requires one "To take all reasonably practical measures to prevent accidents in nuclear installations and to mitigate their consequences should they occur; to ensure with a high level of confidence that, for all possible accidents taken into account in the design of the installation, including those of very low probability, any radiological consequences would be minor and below prescribed limits; and to ensure that the likelihood of accidents with serious radiological consequences is extremely low." And further: "The Safety analysis examines: (1) all planned normal operational modes of the plant; (2) plant performance in anticipated operational occurrences; (3) design basis accidents; and (4) event sequences that may lead to a severe accident". It is specified that "A safety analysis of the plant design shall be conducted in which methods of both deterministic and probabilistic analysis shall be applied". The objective of both analyses are further specified in the Requirements document and more detailed guidance is given in the supporting Safety Guide on "Safety Assessment and Verification" [7].

Regarding probabilistic targets, the Safety Guide refers to INSAG-3 [8] and INSAG-12 [9] and states the following: "Safety function or safety system failure probability: Probabilistic targets can be set at a safety function or a safety system level. These are useful to check that the level of redundancy and diversity provided is adequate. Such targets will be plant design specific, so no guidance is provided here. The safety assessment should assess that these targets have been met.

Core damage frequency: For core damage frequency (CDF), INSAG-3 has proposed the following objectives:
—10^{-4} per reactor year for existing plants,
—10^{-5} per reactor year for future plants.

This is the most common measure of risk since most NPPs have at least a level 1 PSA. In many countries, these numerical values have been used as probabilistic safety criteria (PSC), both formally and informally.

Large release of radioactive material: A large release of radioactive material, which would have severe implications for society and would require the off-site emergency arrangements to be implemented, could be specified in a number of ways, including the following:

- Absolute quantities (in Bq) of the most significant nuclides released,
- As a fraction of the inventory of the core,
- A specified dose to the most exposed person off-site,
- As a release giving "unacceptable consequences".

PSC have also been proposed by INSAG-3 for a large radioactive release. The following objectives are given:

—10^{-5} per reactor year for existing plants,
—10^{-6} per reactor year for future plants.

It is noted in the Safety Guide that instead of this PSC, INSAG-12 states that "**Another objective for these future plants** is the practical elimination of accident sequences that could lead to large early radioactive release, whereas severe accidents that could imply late containment failure would be considered in the design process with realistic assumptions and best estimate analysis so that their consequences would necessitate only protective measures limited in area and in time."

Health effects to members of the public: INSAG has given no guidance on the targets for health effects for members of the public. In some countries, the target for the **individual risk of death** is taken to be 10^{-6} per reactor year for members of the public."

The draft IAEA guide on "The Format and Content of Safety Analysis Reports for Nuclear Power Plants"[10] specifies that a PSA should be incorporated as a chapter of a Safety Analysis Report.

2.1.1.2. Operational safety

A similar trend can be observed with regard to operational safety. The IAEA Requirements for safe operation of NPPs [11] explicitly require the use of PSA for input to the PSR to provide insight into the relative contributions to safety of different aspects of the plant. The Safety Guides supplementing the Requirements for operation recommend using probabilistic methods and approaches as a reasonable tool to ensure the observance of the safety requirements in different areas of the operation of NPPs. Probabilistic assessment methods together with operating experience are recommended for the optimization of the operational limits and conditions and for the justification of their modifications. It is recommended that the frequency of the surveillance activities at a power plant is justified based on a reliability analysis including, where available, a PSA methodology.

Reference [11] states that "Data on operating experience shall be collected and retained for use as input for the management of plant ageing, for the evaluation of residual plant life, and for probabilistic safety assessment and periodic safety review."

The Safety Guide on operational limits and conditions (OLCs) and operating procedures [12] recommends that "Consideration should be given to PSA applications in the optimization of OLCs. Probabilistic assessment methods together with operating experience may be used for justification and modification of OLCs." It is further suggested that "The allowable periods of inoperability and the cumulative effects of these periods should be assessed in order to ensure that any increase in risk is controlled to acceptable levels. Methods of probabilistic safety assessment or reliability analysis should be used as the most appropriate means for this purpose. Shorter allowed outage times than those derived from PSA may be stipulated in the OLCs on the basis of other information such as pre-existing safety studies or operational experience." Also "The surveillance programme should be adequately specified to ensure the inclusion of all aspects of the limits or conditions. The frequency of the surveillances should be stated and should be based on a reliability analysis including, where available, a PSA and a study of experience gained from previous surveillance results or, in the absence of both, the recommendations of the supplier."

Regarding maintenance, it is recommended to optimize the maintenance programme based on the PSA and operating experience. This optimization should ensure that there is a correct balance between preventive maintenance, predictive maintenance, maintenance during power operation or "on-line maintenance" and minimization of breakdown maintenance on safety systems.

The Safety Guide on the qualification and training of NPP personnel [13] recommends training appropriate categories of the plant personnel engaged in the emergency preparedness plan to use all available insights including the PSA evaluation to set priorities for the corrective measures.

Thus, a consensus seems to be emerging that an integrated approach using deterministic engineering principles and probabilistic methods and results is a powerful approach to decision making at NPPs. As a national example, in its Probabilistic Risk Assessment (PRA) Policy Statement [14], the United States Nuclear Regulatory Commission (USNRC) stated "…PRA methods and data should be used in a manner that complements the USNRC's deterministic approach and supports the USNRC's traditional defence-in-depth philosophy". Advocating the use of PSAs in regulatory matters, the same Policy Statement maintains the following: "PRA and associated analyses (e.g. sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state of the art, to reduce conservatism associated with current regulatory requirements, regulatory guides, licensee commitments, and staff practices."

2.1.2. 'Living PSA' as a tool to support risk informed decision making

It is generally recognized and accepted that one important prerequisite for successful PSA application is the availability of a high quality 'living PSA'. Many PSAs in the world have already been maintained as a living PSA framework. It is recognized that the resources dedicated to the living PSA should be coherent with the importance of this work among all the other safety analyses of the plant.

According to a definition from Ref. [15]:

> "*A 'Living PSA' (LPSA) can be defined as a PSA of the plant, which is updated as necessary to reflect the current design and operational features, and is documented in such a way that each aspect of the model can be directly related to existing plant information, plant documentation or the analysts' assumptions in the absence of such information. The LPSA would be used by designers, utility and regulatory personnel for a variety of purposes according to their needs, such as design verification, assessment of potential changes to the plant design or operation, design of training programmes and assessment of changes to the plant licensing basis.*"

The above definition implies that, at the initiation of the LPSA project, the documentation associated with the work performed in each task and the project as a whole must be designed to meet two basic requirements:

- The basis for the LPSA model should be comprehensively documented so that each aspect of the model can be directly related to existing plant information or to the analysts' assumptions of how the plant and the operating staff behave.
- It must be possible to update the LPSA as changes are made to plant design and operation, feedback is obtained from internal and external operational experience, the understanding of thermal–hydraulic performance or accident progression is improved, and advances are made in modeling techniques.

Regarding updating, the following recommendation applies: 'The LPSA should be updated **as frequently as necessary** to ensure that the model remains an accurate representation of the safety of the plant. However, continuous updating of the LPSA appears not to be practicable due to reasons such as control of changes, control of documentation and resources required. It is necessary to assess the impact of any modification (design, procedures, operating practices, licensing basis, etc.) on the PSA in order to check its continuing validity and thus to identify any need for updating. While it is likely that each modification will be assessed on a case by case basis, it would be good practice not to accumulate a backlog of such assessments for a period longer than **one year**. Modifications that significantly impact the PSA results may require an immediate updating of the LPSA. However, even if this type of modification does not arise for a longer period, it is still suggested that the updating process **be audited every three years** and the LPSA formally amended at that time.'

Most Member States have no specific requirements for updating the PSA to represent the "as built, as operated" (US concept) plant. Often the updating is related to the refuelling cycle and on a longer time frame than one year as suggested in the IAEA document.

The quality of the living PSA depends on a well developed and maintained quality assurance (QA) programme that is effectively applied during all PSA phases. The success of developing a living PSA directly depends on the initial QA measures taken. Inadequate QA measures employed in the early stages of a PSA may lead to loss of information and may severely limit the usefulness of the PSA.

Changes in PSA models, data, information and results, including changes to requirements, scope and objectives and input data, should be made in a controlled manner. The reason for a change has to be documented and consideration needs to be given to the impact and implications of the change. When carrying out a change, in principle, the modifications should be handled in the same way as for carrying out the complete PSA (information control; configuration control; documentation control; verification and validation; review). This is a key point for the periodic updating of a living PSA. It might be practical for the updating periods to relate to the length of the refueling cycles.

2.1.3. Safety/risk monitor as a tool to support risk informed decision making

Some PSA applications require the on-line use of the PSA models, and near-prompt knowledge of the instant risk at any time. This requirement can be satisfied by using a special tool called a safety monitor.

Reference [15] defines the safety/risk monitor as follows: "*A Safety Monitor (also referred to as risk monitor) is a plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components. At any given time, the safety monitor reflects the current plant configuration in terms of the known status of the various systems and/or components, e.g., whether there are any components out of service for maintenance or tests. The safety monitor model is based on, and is consistent with, the LPSA. It is updated with the same frequency as the LPSA. The safety monitor is used by the plant staff in support of operational decisions.*"

Since actual plant operation is dynamic, the risk associated with the plant at any particular time during the year may be different from the average annual risk. The safety/risk monitor provides risk based input for plant configuration management in 'real time', including the evaluation of equipment outages and the combined impacts from the actual plant configuration. This information is useful for maintenance prioritization and for the development of contingency plans during unexpected equipment failures. The safety/risk monitor may provide rapid insights about the potential significance of operational events and precursors, provided that these events are within the scope and limitations of the safety/risk monitor models and assumptions.

Safety/risk monitors vary in scope, level of detail and implementation. For example:

- Some plants only include internal events in their risk monitor. Other plants include internal events and some external events.
- Few plants do quantitative risk monitoring during non-power conditions.
- Few plants consider any impacts beyond the equipment out of service. Other time varying factors such as the condition of operating equipment and plant trip potential are often not systematically quantified.
- The identification of the action thresholds varies significantly between plants both in the quantitative values used and in the philosophy of how they are established.
- Most, but not all, plants have found that effective risk monitoring requires a combination of quantitative and deterministic (defence in depth) considerations.

Risk monitors have many limitations which are often ignored and may not be obvious when these tools are put in the hands of a plant operator. This is further explored in Ref. [16].

The number of risk monitors in use at NPPs has been growing rapidly over the past few years. Experience with their use in the day-to-day decision making process has shown that it is possible to manage the risk in such a way that the peaks in the risk have been reduced in magnitude and duration and there is a significant reduction in the average risk.

2.2. WORK BEING DONE BY MEMBER STATES, THE AGENCY AND OTHER INTERNATIONAL ORGANIZATIONS TO ADDRESS REMAINING ISSUES

2.2.1. Efforts to standardize PSA methodology

State of the art PSA methodology is based on a mixture of national and international guidelines, reference PSAs, databases, scientific reference materials and use of commercially available computer tools. It is based on the 'fault/event tree' techniques developed in WASH 1400 [2]. In the absence of a 'PSA standard' the well documented WASH 1400 study was used as a reference study and its principle methodology and some of the data are still being used today. As a basis for staff training a fault tree handbook [17] was issued and internationally widely distributed by the IAEA in its efforts to promote the use of PSA and to assist its Member States in carrying out PSA studies. More detailed guidance was then provided in the USNRC Procedures Guides [18,19]. At the international level the IAEA has prepared a series of guidance documents [20—27]. Other major efforts to harmonize PSA methodology are published in Refs [3, 28]. Based on the various broadly consistent guidance documents, many countries have developed their own national guidance. The degree to which they are prescriptive varies, as does the use a country makes of PSA.

From the beginning it was recognized that peer review was an important aspect of ensuring the quality of PSAs. This contributed to reaching a high standard. At the international level the IAEA has been carrying out International PSA Review Team (IPSART) missions (earlier known as IPERS). Specific guidelines for such review missions have been prepared [29] and they use as a reference the IAEA guidance documents and good international practices.

IPSART reviews of PSAs have frequently identified a lack of a rigid QA process in general and lack of adequate documentation in particular. This is making the peer review very difficult and hinders maintaining the PSA as a living document. It also hinders the review by the regulatory organization and thus reduces its effectiveness for decision making. The IAEA has therefore prepared guidance for QA in carrying out PSAs [30], which includes guidance on PSA model configuration management. The requirements of documentation have been specified in a document providing guidance for regulatory review of PSAs [31,32]. Guidance on documentation management for 'living PSAs' is provided in Ref. [15].

Within its IPSART programme the IAEA has performed numerous PSA reviews. Regarding the scope it has been found that in addition to the level of PSA performed and whether or not low power and shutdown states are included, the main differences relate to the treatment of:

—Internal fires and floods (including the 'turbine hall effect'),
—External events, in particular seismic events,
—Accident Management measures.

With regard to the quality of PSAs, in addition to the issue of documentation and quality control, the main differences relate to the treatment of:

—Large pipe break frequencies,
—Steam generator tube rupture,
—Definition of LOCA success criteria,
—Pump seal failures,
—ATWAS sequences,
—HF modelling,
—Modelling of recovery actions,
—Modelling of CCFs (including IEs).

In the absence of detailed prescriptive standards, the IAEA guidance on the regulatory review of PSAs recommends that at the start of preparing a PSA, agreement is reached with the regulatory body on the exact scope of the study and on acceptable methodologies. The advantage of a non-prescriptive approach is the flexibility provided in encouraging the development of new methodologies. The disadvantage may be the need for a more difficult and detailed review process.

A recommendation on whether to standardize PSA at this time needs to take into account the impact it will have on the existing PSAs, which have been used for years. A standardization effort would need to be justified by a comprehensive analysis of the real necessity for changes in methods and data. It also needs to be considered that requirements from different regulators in different countries (level of detail, level of review, etc.) could lead to different conclusions and applicability of results.

The major ongoing activities in these areas, external to the IAEA, include the development of a draft PSA standard by the ASME [33] and the PSA peer review (certification) process developed by the US nuclear industry. Development of the US industry PSA peer review process was initiated by the US Boiling Water Reactor Owners Group (BWROG) and has been adopted for use by the other US NPP owners groups.

2.2.1.1. BWROG certification process

The overall objectives of the BWROG certification process [34] are to assess PSA quality and determine its adequacy for use in assessing specific applications. It is currently applicable to Level 1 and Level 2 PSAs. Certification is something of a misnomer, since no certificate is issued. A better description is a detailed expert peer review process.

The overall PSA quality is not graded (but can be inferred from reviewing the major element grades). The concept is to allow identification of the major PSA elements (and subelements) required to support a specific application and to assess the quality of the PSA in these required areas. For each application the impacted portions of the PSA are to be identified (i.e. elements and subelements) and the scores for these aspects of PSA are reviewed and compared with the required quality grade identified for the application.

The following provides a short summary of the grading used:

—Grade 1: This grade corresponds to the attributes needed for identification of plant vulnerabilities, i.e. responding to USNRC Generic Letter 88-20. A PRA with mostly Grade 1 elements is considered acceptable for:

- Satisfying the GL 88-20 requirement,
- Assessing severe accident vulnerabilities,
- Resolving selected generic issues (e.g. A-45),
- Prioritizing licensing issues

—Grade 2:
This corresponds to the attributes needed for the risk ranking of systems, structures, and components. Examples of such applications include the following:

- MOV ranking for GL 89-10,
- USNRC inspection activities,
- Maintenance rule support.

—Grade 3 This review grade extends the requirements to ensure that risk significance determinations made by the PRA are adequate to support regulatory applications, when combined with deterministic insights. Examples may include the following:

- Graded QA,
- In-service testing (IST),
- In-service inspection (ISI),
- Backfit calculations (see also Grade 4),
- Reduced or eliminated licensing commitments,
- On-line maintenance evaluations,
- Single TS changes.

—Grade 4: This review grade requires a comprehensive, intensively reviewed study that has the scope, level of detail, and documentation to ensure the highest quality of results. Routine *reliance* on the PRA as the basis for certain changes is expected as a result of this grade. Examples may include the following:

- Reduced or eliminated licensing commitments (sole basis),
- Modify Technical Specifications (sole basis)
- Replace Technical specifications with an on-line risk monitor,
- Backfit calculations,
- Reclassification of the quality category of some equipment

It should be noted that a PRA would not require all subelements to receive a grade 3 in order to be used for a grade 3 application. Rather, subelement grades less than 3 would require an assessment to determine the impact.

2.2.1.2. ASME standard for PRA for nuclear power plant applications

A recent effort by ASME is devoted to developing a PSA Standard [33] In 1998 in the USA a Standards Committee was formed to develop a national PSA standard to serve as a basis for risk-informed applications containing the requirements for PSAs to be applied, and prescribing and adapting these requirements for specific applications. The draft ASME PSA standard has already been prepared and is under discussion at several forums.

Since the standard is intended for a wide range of applications, corresponding capability categories have been defined. Applications vary with respect to which risk metrics are employed, which decision criteria are used, the extent of reliance on the PRA results in supporting a decision, and the degree of resolution required of the factors that determine the risk significance of the proposed changes. Each application is then evaluated by considering these attributes.

The draft standard states that "Depending on the application, the required level of PRA capabilities may vary over different elements of the PRA, within a given element, across different accident sequences or classes of accident sequences, initiating events, basic events, end states, and operating modes. While the range of capabilities required for each part of the PRA to support an application falls on a continuum, three Capability Categories are defined in this Standard so that requirements can be developed and presented in a manageable way. They are designated as PRA Capability Categories I, II, and III". The attributes of a PRA for each of these Capability Categories are summarized in Table III from this draft standard. For each element of a PSA the Standard defines "High Level Requirements" that are the same for all applications, and "Supporting Requirements" (SRs) which are differentiated by Capability Category.

It is recognized that "the boundaries between these Capability Categories are arbitrary. When a comparison is made between the capabilities of any given PRA and the SRs of this Standard, it is expected that the capabilities of a PRA's elements or parts of the PRA within each of the elements will not necessarily all fall within the same Capability Category, but rather will be distributed among all three Capability Categories. Indeed, there may be PRA elements, or parts of the PRA within the elements that fail to meet the SRs for any of these Capability Categories".

The Standard also contains the requirements for the PSA configuration control, i.e. how to conduct a "Living PSA" programme.

TABLE III. BASES FOR PRA CAPABILITY CATEGORIES (FROM DRAFT ASME STANDARD MATERIALS)

Criteria	Capability Category I	Capability Category II	Capability Category III
1. *Scope and level of detail:* The degree to which resolution and specificity are incorporated such that the technical issues are addressed.	Resolution and specificity sufficient to identify the relative importance of the contributors at the system or train level including associated human actions.	Resolution and specificity sufficient to identify the relative importance of the contributors at the SSC including associated human actions level, as necessary (see note a).	Resolution and specificity sufficient to identify the relative importance of the contributors at the subcomponent level including associated human actions, as necessary (see note a)
2. *Plant-specificity:* The degree to which plant-specific information is incorporated such that the as-built and as-operated plant is addressed.	Plant-specific information sufficient for the model to account for the unique design and operational features of the plant.	Plant-specific information sufficient for the model to reflect the as-built and as-operated plant (see note b).	Plant-specific information sufficient. for the model to match (or duplicate) the as-built and as-operated plant (see note b).
3. *Realism:* The degree to which realism is incorporated such that the expected response of the plant is addressed.	Departures from realism will have moderate (conservative or acknowledged, potential non-conservative) impact on the conclusions and risk insights as supported by good practices (see note c).	Departures from realism will have small impact on the conclusions and risk insights as supported by good practices (see note c).	Departures from realism will have negligible impact on the conclusions and risk insights as supported by good practices (see note c).

NOTES:

(a) The definition for Category II is not meant to imply that the resolution and specificity are to a level to identify every SSC and human action. Similarly, for Category III, it is not meant to imply that the resolution and specificity are to a level to identify every subcomponent for every component.

(b) The differentiation between "account for", "reflect" and "match" (or "duplicate") is the level of confidence that the model represents the as-built and as-operated plant. In Category I, the model should incorporate realistic or conservative representations of significant features. In Category II, the model should incorporate realistic representations of modelled SSCs consistent with current good practices. In Category III, the model should incorporate accurate representations of modelled SSCs to the extent practical.

(c) Differentiation from moderate (conservative or acknowledged, potential non-conservative), to small, to negligible is determined by the extent to which the impact on the conclusions and risk insights could affect a decision under consideration. This differentiation recognizes that the PRA would generally not be the sole input to a decision. A moderate impact implies that the impact (of the departure from realism) is of such sufficient size that it is likely that a decision could be affected; a small impact implies that it is unlikely that a decision could be affected, and a negligible impact implies that a decision would not be affected.

2.2.1.3. IEC Standards

The International Electrotechnical Commission (IEC) issued in its Standard series the International Standards No. 61508 [35] and No. 300-3-9 [36], dealing with the requirements for risk analysis and functional safety analysis of technological systems specifying the scope of the analysis in general. They intend to provide guidelines for selecting and implementing risk analysis techniques for risk assessment of technological systems. The objective of these standards is "to ensure quality and consistency in the planning and execution of risk analyses and the presentation of results and conclusions." It lists the tasks to be performed when carrying out the risk analysis.

2.2.2. Risk informed regulations

There are several examples where, on a voluntary basis, plants in the USA have chosen to make use of the "risk informed" approach to reach relaxation from present specifications. Table IV summarizes the use of risk information in USNRC and industry programmes [37] and demonstrates the emphasis given to this approach by various institutions in the USA.

'Risk informed' is part of an integrated decision making process, which includes the need to:

- Comply with the current regulations.
- Maintain the defense in depth approach, i.e. meet deterministic requirements for redundancy, diversity, separation, segregation, equipment qualification, etc.
- Provide for adequate safety margins.
- Demonstrate risk reduction, risk neutral or a small increase in the risk measure.
- Monitor subsequent performance.

The approach includes key comparisons of 'at power', 'transition', or 'shutdown (or mode specific)' risks. Such applications may include the use of compensatory measures, e.g. ensuring the availability of certain systems while performing test or maintenance on the system under consideration for relaxation of specifications.

In the area of in-service inspection, pilot studies at the Surry, Vermont Yankee and Arkansas Nuclear One NPPs have shown an overall risk benefit by reducing personnel radiation exposure, by ensuring that inspection activities focus on piping segments with important degradation mechanisms or high failure consequences.

In the area of in-service testing, several studies have led to an adjustment of test frequencies for pumps and valves by categorizing them into those of high or low safety significance, partly under the constraints of ensuring compensatory measures during the tests. A full scope revision programme for the Comanche Peak NPP has shown an increase in CDF of less than 10^{-6} per year which, at a qualitative level, was decided to be risk neutral. It led to adding risk important components to the programme, but led to fewer tests and thus fewer realignment errors.

A pilot South Texas project in the area of graded quality assurance demonstrated that QA efforts could be reduced in a risk neutral application; however, implementation was complicated by other existing regulations.

Regarding the acceptance of risk informed decisions, presently there are two acceptance guidelines applied at the USNRC [38], one for CDF and one for Large Early Release Frequency (LERF), *both* of which should be used. The guidelines for CDF are illustrated by Fig. 1 and the guidelines for LERF by Fig. 2.

TABLE IV. USE OF RISK INFORMATION IN USNRC AND INDUSTRY PROGRAMMES

CDF/ DCDF	**RG 1.174 Low CDF/LERF**	**RG 1.174 High CDF/LERF**	**EPRI PSA Application Guide**	**EPRI Temp. Change**	**OL 803**	**Oversight Process SECY-99-007**	**RAG Screening Criteria**	**NEI 91-04 Severe Accident Guidelines**	LERF/ DLERF
10^{-3}									10^{-4}
			"Unacceptable"			"RED" "Unacceptable"	"Proceed to Value Impact Analysis" (PRIORITY)	"Cost Effective Admin. Procedure or Hardware Change" or "Treat in EOP" or include in SAMG	
10^{-4}	"Not Normally Allowed"	"Not Normally Allowed"		"Potentially Risk Significant"	"Substantial Risk Significance"				10^{-5}
			"Further Evaluation Needed"			"YELLOW" "Required Reg. Response"	"Proceed to Value Impact Analysis"	"Cost Effective Admin. Procedure or Hardware Change" or include in SAMG	
10^{-5}									10^{-6}
	"Small Changes" (Acceptable w/Management Attention			"Assess Non-Quantifiable Factors"	"Low to Moderate Risk Significance"	"WHITE" "Increase Reg. Response" . . .	"Value Impact Analysis upon Management Decision"	"Include in SAMG"	
10^{-6}									10^{-7}
	"Very Small Changes" (Acceptable)	"Very Small Changes" (Acceptable)	"Non-Risk Significant"	"Non-Risk Significant"	"Very Low Risk Significance"	"GREEN" "Routine Reg. response"	[No Action]	"No Specific Action Required"	
10^{-7}									10^{-8}

These guidelines are intended to provide assurance that proposed increases in CDF and LERF are small and are consistent with the intent of the Commission's Safety Goal Policy Statement.

These criteria are quite complex in their structure. The regulatory guide further specifies that the acceptance guidelines are to be compared to mean values. However, it is recognized that not all sources of uncertainty are evaluated quantitatively in PSAs. Thus it has been stated as a requirement that the way in which the decision is to be made hinges on whether there are sources of uncertainty that might affect the decision.

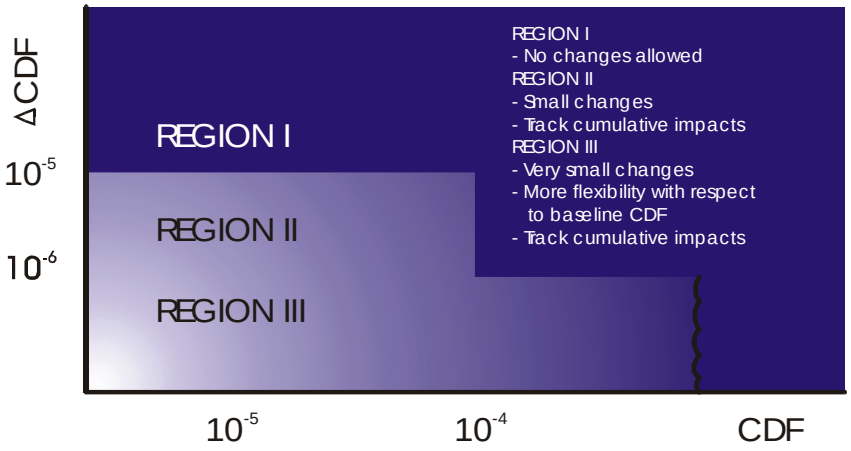

FIG. 1. Acceptance guidelines for CDF.

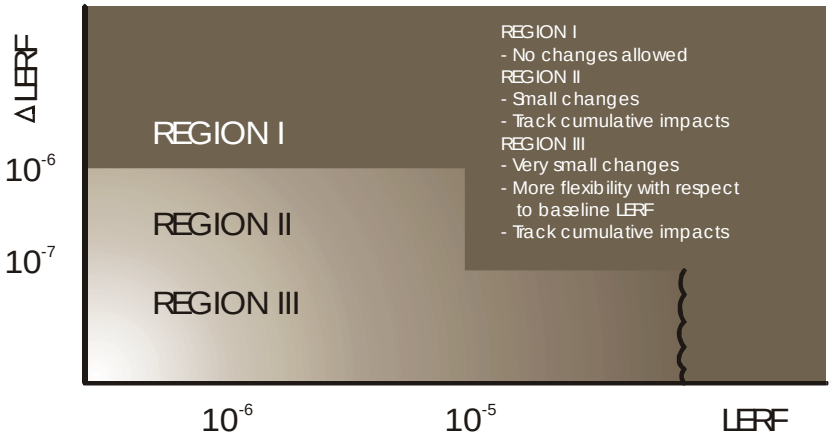

FIG. 2. Acceptance guidelines for Large Early Release Frequency (LERF).

The White Paper on Risk-informed and Performance-based Regulation [39] shows the evolution of the USNRC approach to regulatory decision making from the traditional prescriptive approach based on deterministic safety assessment through the risk based approach, the performance based approach to the risk informed and performance based approach. The selection of the new approach started with acknowledging the improvements in the performance of the nuclear industry in the USA, moving from prescriptive to performance based regulatory approach and "risk-informing", i.e. including risk based considerations into the new regulatory process.

The USNRC has started the 'New NRC Reactor Inspection and Oversight Program' [40], introducing the latest approach to the regulation of the nuclear industry. This is the risk informed, performance based approach to regulation that has been discussed in several forums over the last years. One key area in this approach is the monitoring of the safety performance of NPPs, and the consequent basing of regulatory actions on the actual safety performance. The basis for monitoring safety performance was the identification of "cornerstones" of safe nuclear plant operation by performance indicators, each categorized to determine the appropriate regulatory response. The 'Significance Determination Process' supports the reactor oversight programme by determining the safety significance of inspection findings and performance indicators, as indicated in Table V.. Presently the approach is applied in all plants, and the first end-of- cycle performance reviews are being evaluated. The development and use of such indicators is explored in detail in Topical Issues Paper No. 5.

2.2.3 Regulatory approach in the UK

In the UK, the legal requirement given in the Health and Safety at Work Act, 1974 [41] and the Nuclear Installations Act [42] is that risk must be reduced "so far as is reasonably practicable" (SFAIRP) — that is, to a level that is "as low as reasonably practicable" (ALARP).

Guidance for the application of the ALARP principle is given in the "Tolerability of Risks from Nuclear Power Plants" [43] — referred to as ToR. This sets out the framework used for controlling risks at NPPs and introduces the concept of three levels of risk as follows:

- An *unacceptable region* where risks cannot be justified;
- A *tolerable region* where measures must be taken to control the risk and to ensure that they are ALARP; and
- A *broadly acceptable region* where the regulator would not press for further safety improvements to be made to reduce the risk.

The "Safety Assessment Principles for Nuclear Plants" [44] uses this framework and defines basic safety limits (BSLs) and basic safety objectives (BSOs), which are defined for a number of measures of risk. For example, for the frequency of plant damage (which relates to core damage frequency for a reactor) the BSL is defined as 10^{-4} per year and the BSO as 10^{-5} per year. For the large release frequency, the BSL is defined as 10^{-5} per year and the BSO as 10^{-7} per year.

A further publication, “Reducing Risks, Protecting People”, issued for public comments in 1999 [45], broadens the framework for regulating the risk from NPPs so that it can be applied to other industrial activities.

The ALARP requirements mean that an employer must do whatever is reasonable practicable to reduce risks. In legal terms, this means that improvements need to be made unless their cost grossly exceed the reduction in risk. Although formal cost–benefit techniques can be used to assist in making these judgements, this is not generally done in the UK nuclear industry.

Table V. USNRC MODEL FOR EVALUATING LICENSEE PERFORMANCE INDICATIONS

- GREEN -
(ACCEPTABLE PERFORMANCE — Licensee Response Band)

— Cornerstone objectives fully met
— Nominal Risk/Nominal Deviation From Expected Performance

- WHITE -
(ACCEPTABLE PERFORMANCE -- Increased Regulatory Response Band)

-- Cornerstone objectives met with minimal reduction in safety margin
-- Outside bounds of nominal performance
-- Within Technical Specification Limits
-- Changes in performance consistent with ΔCDF<E-5 (ΔLERF<E-6).

- YELLOW -
(ACCEPTABLE PERFORMANCE - Required Regulatory Response Band)

-- Cornerstone objectives met with significant reduction in safety margin
-- Technical Specification limits reached or exceeded
-- Changes in performance consistent with ΔCDF<E-4 ΔLERF<E-5)

- RED -
(UNACCEPTABLE PERFORMANCE - Plants not normally permitted to operate within this band)

-- Plant performance significantly outside design basis
-- Loss of confidence in ability of plant to provide assurance of public health and safety with continued operation
-- Unacceptable margin to safety

---

3. PROBLEMS IDENTIFIED, ISSUES TO BE RESOLVED

3.1. REQUIREMENTS OF PSAS FOR USE IN RISK INFORMED DECISION MAKING

Recent developments in a number of countries include expanded utilization of PSA methods and results in risk informed decision making, risk informed operations and regulatory oversight. The main driving force behind this movement is the perception that the use of risk insights can result in both improved safety and a reduction in unnecessary regulatory requirements; hence leading to a more efficient use of the resources of NPP operators and the regulatory authority.

These expanded uses of a PSA place increased demands on the quality and consistency of the PSA. Key questions that arise are: How does one assess quality in a PSA? How much quality is required? How does one assure consistency?

3.1.1. PSA quality

Judgments on the quality of a PSA are by their nature subjective. However, they are facilitated by clearly defined requirements regarding PSA methods, assumptions, and documentation. In addition, a rigid QA process needs to be followed, which also extends to the management of maintaining a 'living PSA'. Furthermore, a clearly defined process for independent peer review to assess PSA quality is critical.

The **PSA quality should be commensurate with its intended application**. This means that there is not one standard for judging the adequacy of a PSA but that the quality of the PSA must be judged in relation to each specific use or application.

Questions of consistency involve both internal and external aspects. Internal consistency relates to the coherence of PSA methods, assumptions, and documentation throughout a specific PSA. External consistency involves these considerations among PSAs for plants of similar design classes. Consistency is fostered by establishing requirements and guidance for performing PSAs, by a structured peer review process and by cross-comparisons of PSAs for similar (and different) designs.

As suggested in the above discussion the key elements of quality in PSAs are clearly defined requirements and guidance (standards), strictly followed QA procedures and a structured peer review process.

3.1.2. Treatment of uncertainties

An important element of risk informed decision making is adequate consideration of uncertainties. There are two types of uncertainty in PSAs: quantifiable and non-quantifiable uncertainty. Quantifiable uncertainties are related to the random statistical behaviour of equipment failures characterized by a statistical distribution, and to the lack of information to form statistical data in case of rare events characterized rather by assumed distribution function with confidence interval. The advantage of the PSA compared with deterministic studies is that these uncertainties can be evaluated and quantified by rigorous propagation of the basic uncertainties through the model.

On the other hand the uncertainties that are associated with modelling and completeness cannot be quantified. These uncertainties are mostly related to the assumptions made during modelling. They can be evaluated by sensitivity calculations in order to determine the effect of the variations of the assumptions on the PSA results, and consequently on the risk informed decision.

The uncertainties increase with the level of PSA. At higher levels of PSA the role of the assumptions increases and the study includes analyses of the structural behaviour of the containment, or factors like aerodynamic dispersion of radioactive material that further increase the earlier mentioned uncertainties.

Consideration of the uncertainties cannot be avoided independent of the case deterministic or probabilistic approach. This should be taken into account when making risk informed decisions. They have to be analysed instead. The propagation of the uncertainties of the numerical values of the input data towards the PSA results should be analysed, quantified and documented. The non-quantifiable uncertainties should be analysed by sensitivity calculations in order to determine the influence on the PSA results. Probabilistic safety criteria should be defined in such a way as to take into account the uncertainties.

3.1.3. International PSA standards

In the absence of prescriptive PSA standards there are two complementary ways of ensuring quality and consistency. One possibility is to subject a well documented and available PSA for a certain category of NPP design to a high degree of peer review and then to use this as the reference PSA. Prominent examples of this approach are the WASH-1400, NUREG-1150, the German Risk Study or EPS-900 and EPS-1300. Another possibility is to establish user groups for similar types of plants and to compare PSA results and analyse the differences. Such user groups have, for example, been established to compare the individual plant examinations (IPEs) in the USA. The IAEA is promoting both approaches by, for example, establishing such groups for PHWRs and for different types of WWER reactors. In addition the IAEA is promoting peer review through its IPSART service. Efforts have been started in Nordic countries to compile information on PSA studies on a CD-ROM, to be available as a reference to those who are performing or reviewing PSAs.

It thus needs to be discussed if at this stage of affairs it is desirable to develop international standards for PSAs.

3.1.4. Peer reviews

At present the activities of IAEA Member States regarding peer reviews of PSAs and PSA applications vary from country to country. As stated earlier, States with several NPPs have specific approaches, including procedures for regulatory review. Some countries request external peer review teams (such as IPSART) to complement national efforts.

Peer reviews serve as a part of the QA process. A typical high level peer review team would consist of five to six experts not involved into the development of the PSA, and the process would cost a 12–15 expert-week effort. Since the peer review cannot cover all the details of the PSA, a full review would involve much more effort. Depending on the licensing approach in the country, the regulatory review can be a full detailed review, or also a reduced scope peer review. It reflects the needs for expertise to support this regulatory activity.

There is a tendency to perform a peer review of the PSA applications, including the usability of the PSA for the specific application. The ASME Standard mentioned earlier specifies the requirements and scope for such a review. Also, the IAEA extended its IPSART programme with peer review missions on PSA applications.

At the OECD/NEA–CNRA "Special Issues" meeting in 1997, it was recognized by the senior regulators that formal guidance for the regulatory review of a PSA did not exist. A recommendation was made that such guidance needed to be produced to establish an agreed basis for assessing whether important technological and methodological issues were being treated adequately, and to verify that the conclusions reached were appropriate. This guidance is being produced by the IAEA in co-operation with the OECD/NEA [31, 32]. These documents raise issues about how the review should be carried out, such as the timing of the review (on-line or off-line), the extent/level of detail of the review and the range of expertise required.

3.2. PROBABILISTIC SAFETY GOALS, ACCEPTANCE CRITERIA

If PSA results are to be used in a formal way for decision making, then it is necessary to establish a formal process for using those results. The details of this process will depend on the purpose of the particular PSA application, the nature of the decision, and the PSA results to be used. When the numerical results of the PSA are to be used, it will often be necessary to establish some reference value with which those results can be compared, as well as a rule, or rules, for how to interpret the results of the comparison. Where the risk informed application is directed towards the identification of the dominant contributors to risk or the optimization (minimum risk) among various design options, plant configurations, testing strategies, etc., there may be no need for a reference value at all. Such uses of PSA, depending only on a relative ranking of values, are often claimed to be the most robust. However, where the application involves judging whether a calculated risk value is acceptable, assessing the acceptability of a proposed change to the plant that would produce a calculated increase in risk, or assessing the need for a change in design or operational practices to reduce the level of risk, then a judgment on the significance of the calculated value can only be made by comparing it with some reference value. These reference values and their associated rules are called probabilistic safety criteria (PSC), and sometimes probabilistic safety goals.

The meaning of the numerical value of the PSC and the decision making rule itself will depend very much on its use. Different PSC are adopted for different decisions. The PSC are specified not only by the numerical values proposed, but also by specifying what value, calculated from the PSA, should be used for comparison purposes, and to indicate how to interpret the results of the comparison. As an example, when specifying the safety goals in its Safety Goal Policy, the USNRC specified that the mean values estimated from the PSA were to be compared with the goals, that all contributions to risk were to be considered and that meeting the goal meant that the plants were safe enough.

About ten years ago INSAG-6 [46] concluded that the lack of standardized PSA methodology made it difficult to compare the numerical results of different PSAs. It also concluded that the methodology was not sufficiently mature for its present status to be frozen. But it recognized an emerging international consensus on target probabilities of core damage and large accidental release. The criteria proposed in INSAG 3 [8] and INSAG-12 [9] were discussed above as included in the safety guide on "safety assessment and verification".

The major issues related to probabilistic safety goals and acceptance criteria to solve in the future are the following.

Different countries apply different values for probabilistic safety goals. In many countries no probabilistic safety goals exist. Although there have been many forums to discuss these goals, and there are even standards dealing with probabilistic acceptance criteria, there is no methodological guidance or procedures on how to establish and what should be the basis for a system of probabilistic safety goals that could be recommended internationally.

The calculated uncertainty ranges of the PSA results are sometimes orders of magnitude wide. The way to handle uncertainties in relation to using the values of probabilistic safety goals also differs from country to country. As already stated, some countries use mean values of the calculated results, while others use values including the calculated uncertainties (confidence levels) to compare the probabilistic safety goals.

There are different approaches to the acceptance of complex decisions containing multiple modifications, changes resulting in a risk or risk increase meeting the acceptance criteria. The risk informed assessment can prove the acceptance of such complex decisions; however, it might be that one or more elements of the decision bring alone unacceptable risk or risk increase, while others serving as compensatory measures result in risk reduction.

The definition of a 'risk neutral' decision should be part of the PSC system. A simple example of a risk neutral decision is one that either does not affect the risk, or causes negligible risk increase (e.g. less than 10^{-7} Δ CDF), and therefore will not be controlled by PSC. In some countries the value of the negligible risk increase has already been defined in the framework of their PSC system. More complicated cases include trade-off of positive and negative changes (which is not allowed in the USA to be presented in one package) or shifts in the risk curve if used. There should be an international consensus on the common basis for defining risk-neutral decisions.

3.3. COMPUTER SUPPORT FOR RISK INFORMED DECISION MAKING

A number of computer codes and software packages are currently used for performing a PSA. Typically, an integrated software package is used in Level 1 PSA analyses for the development and storage of system models, sequence models, handling of failure data and sequence quantification. Additionally, other computer codes may be used for the determination of success criteria. Level 2 and Level 3 PSA analyses also require the use of large computer codes. Finally, smaller pieces of software may be used for special analyses, conversion or transport of data. Increasingly, integrated software packages are developed and used covering almost all levels of a PSA.

In order to ensure QA for the PSA, all computer codes used in the development and application of the PSA must be verified and validated, either in the course of their development or by the PSA group. Computer codes that are purchased commercially may be verified and validated by the code developer. For software that is not commercially procured but, for example, written internally in the PSA organization, verification, validation and QA should be established.

3.4. ORGANIZATIONAL FACTORS

An important aspect of risk informed decision making is that it needs to be agreed to which extent the human factors and aspects of safety culture and organizational aspects will be included. Presently, PSAs model human failure and human action of recovery in case of an accident. Usually the human actions for which written procedures exist are given credit in the PSA. There are standard modelling techniques that are applied. These techniques mostly use generic human error probabilities modified by different factors (known as performance shaping factors). These performance shaping factors are characterized by corrective values representing the different factors influencing human behaviour and performance such as the complexity of the task, the human–machine interface, training practice, and the usability of procedures. In an increasing number of PSAs, special human factor studies are applied using the results of the control room crew exercises on the plant simulator. It is good practice to take into account, to the extent possible, plant specific data. Thus, these limited aspects of safety culture and these organizational aspects are taken into account to the extent that they influence human behaviour.

In this regard some experts take the view that organizational aspects should be included in the analysis. Others believe that this is not subject to quantification, adds large margins of uncertainty and opens the door to manipulation of the PSA results. Thus, good safety culture and safety management add an additional layer of protection against accidents which cannot and should not be quantified. In any case consideration of organizational factors in PSAs should be very practical and not resource consuming.

3.5. FUTURE PASSIVE REACTORS

Risk informed decision making plays an important role in the development of future reactors. Such developments have two objectives, increase in safety and reduction of costs, in particular through simplifying safety systems and reducing the requirements for safety classification of safety systems and components. However, specific problems are posed for performing reliable PSAs for such future reactors making more extensive use of highly reliable passive components. The safety of these reactors is challenged by very severe low probability initiating events. The impact of these events is, to a large extent, determined by the phenomenological response of the plant to these events, rather than by a sequence of successes / failures of components / systems, which individually have higher probabilities and which can be analysed and modelled with much less uncertainty due to the existence of a reliable statistical database. In addition, it is necessary to consider much longer mission times for components of, for example, several days in comparison to the usual time of 24 hours. Thus, this poses particular methodological problems for making risk informed decisions for these reactor designs which, however, are expected to pose a much lower risk.

4. RECOMMENDATIONS FOR STRATEGIC ACTIONS / PRIORITIES FOR FUTURE WORK

4.1. STRATEGIC ACTIONS

4.1.1. Role of PSA in nuclear safety

The recently revised IAEA Safety Standards give more emphasis to the role of PSA, particularly in the areas of design, periodic safety review and operational safety. Member States should make use of the advances in PSA methodology to improve safety. To this end, Regulatory Bodies should determine their policy and provide clear guidance on the use of PSA for safety related decision making, on the complementary role of PSA and defence-in-depth and good engineering practice, and establish the related safety standards and legal basis.

In recent years, there has been a greater use of the risk information provided by PSAs in the regulatory decision making process. However, the way that this is being done varies significantly in different Member States, and indeed some regulators are not following a risk informed approach at all.

Hence, there is a need to review experience in risk informed decision making, how this relates to the legal framework that the regulators are working in, and whether this has increased regulatory effectiveness. In addition, it needs to be determined why some Member States have not adopted a risk informed approach.

4.1.2. Living PSAs, risk/safety monitors

In order to benefit from PSA, regulators and operators should strongly support the idea that plant specific living PSAs be available at each NPP and be used as a complementary tool in making safety related decisions. The current trend is for the living PSAs to be developed into risk/safety monitors, which are used by plant operators during NPP operation and by regulatory bodies. There is a need to provide guidance on the development and use of these risk/safety monitors.

4.1.3. Technical correctness

In order to be useful for safety related decisions, the PSA models have to correctly represent the NPP. In order to achieve technical correctness of the results of PSA supported safety decisions, countries should employ quality standards for PSAs related to the intended use, establish user groups for similar types of plants, which can include efforts of pooling of reliability data, promote the availability of reference studies as benchmarks, and encourage peer review, including use of international peer review services such as the IAEA IPSART service.

4.1.4. Regulatory review of PSAs

It is necessary to avoid the use of low quality PSAs for safety decisions. Therefore, Regulatory Bodies should increase their efforts to review PSAs. The Regulatory Bodies need to ensure their technical competence, needed for the review of PSAs and for reviewing and approving safety related analyses and modifications using probabilistic arguments. Guidance documents on regulatory review raise issues, as discussed above, such as the timing of the review (on-line or off-line), and the extent/level of detail of the review.

4.1.5. Probabilistic safety criteria

In order to contribute to regulatory stability and public confidence, Regulatory Bodies should establish clear criteria for the use of PSA results. These criteria concern:

- Probabilistic safety targets/goals for the NPPs;
- Assessment of variations of instant probabilistic measures of the safety level of a plant as obtained from risk/safety monitors (e.g. CD or LERs);
- Configuration control of alignment of systems/components, e.g. for testing and maintenance;
- Measurements of changes of the safety level due to modifications related to design or operation, including the definition of 'risk neutral' and the treatment of multiple changes and compensatory measures; and the
- Treatment of uncertainties or use of confidence intervals in all the above areas.

The recommendations from INSAG have been summarized above. In addition, the issue of defining operational safety criteria which relate to the instantaneous measures of risk produced by risk/safety monitors needs to be addressed. However, there have been a number of developments in the way that risk criteria have been defined and used in Member States, some of which are discussed in Section 3. There is a need to review these developments and to consider whether it would be possible to reach a consensus.

4.1.6. Key uncertainties

PSA is accompanied by uncertainties at all levels of the analysis, which thus have to be taken into account in the decision making process, as discussed in Section 3.1.2. The key uncertainties are mostly related to areas where the lack of knowledge or information causes uncertainties in particular related to phenomenological aspects such as failures of large pipes or other pressure containing components.

Therefore, Member States and international organizations should review the key contributors to the uncertainties in PSAs and compile experience, carry out research where necessary, and provide guidance on how to reduce the uncertainties.

4.1.7. PSAs for future reactors

In order to increase safety, the proposals being made for future reactors make increasing use of passive systems. This poses methodological problems in a PSA since there is less experience in modelling passive systems compared to active systems. For passive systems to work, a number of boundary conditions need to be met —reactor coolant pressure, etc., and the PSA needs to determine the probability that these boundary conditions will *not* be met. In general, it is to be expected that the risk profile of such plants will be significantly different.

It is recommended to review how passive systems are modelled in PSAs and to provide guidance on this topic.

4.1.8. Cost–benefit analysis

A limited number of countries use the results of PSAs within the framework of cost–benefit analysis. It would be useful to compile the experience gained in these countries and to analyse the factors which should be considered.

4.1.9. Wider use of PSA

At present PSA methodology is mainly applied in the area of the safety of NPPs, though some more limited use has been made for research reactors, other fuel cycle installations, isotope production facilities, large irradiation facilities, etc. Guidance [47] has recently been provided for conducting PSAs for non-reactor fuel cycle facilities. For many facilities a simplified approach may be taken. The depth and detail of the analysis should be commensurate with the level of hazard posed by a facility. Due to the wide range of facilities, there are limited generic component reliability data and even less plant specific data available. With due consideration of these limitations, it is nevertheless strongly recommended to make greater use of PSA beyond the NPP applications to identify the vulnerabilities of a facility design or configuration, and critical human actions important to safety.

5. QUESTIONS TO THE CONFERENCE

The questions to the conference can be grouped into the following four areas.

- **Introduction of risk informed decision making in Member States**

5.1. Is there sufficient consensus regarding the introduction of risk informed decision making into nuclear safety? Why are some countries still hesitant?

5.2. Is risk informed regulation increasing regulatory effectiveness?

5.3. Is risk informed regulation of benefit to utilities?

5.4. Are regulators prepared to review PSAs and PSA applications? How much effort is needed?

- **Criteria to be used in 'risk informed' decision making**

5.5. What PSC are needed to facilitate risk informed regulation? Is there a sufficient legal basis for risk informed decision making?

5.6. Is it possible to define 'risk neutral' decisions?

5.7. Why is there no international agreement on PSC? Is international agreement wanted? What should be done to reach agreement?

- **Quality of PSAs as a basis for 'risk informed' decision making**

5.8. Is there sufficient guidance for the preparation of high quality PSAs? Is there a need for an international standard for PSAs?

5.9. Is PSA methodology sufficiently developed to support 'risk informed' regulation, e.g. treatment of rare events, modelling of human failure, severe accident management, organizational factors? Is PSA methodology sufficiently developed to model new reactor designs more dependent on passive safety features?

5.10. How is it possible to ensure that operators are in a position to develop, use and maintain living PSAs and risk/safety monitors to support 'risk informed' decisions?

- **International co-operation**

5.11. What actions should be taken by the IAEA to support the introduction of 'risk informed' decision making, e.g. related to the areas of development of international standards, harmonization of criteria, compilation and dissemination of experience, and education and training?

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, IAEA-TECDOC-1200, IAEA, Vienna (2001).

[2] UNITED STATES NUCLEAR REGULATORY COMMISSION, Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants, WASH-1400-MR (NUREG-75/014), USNRC, Washington, D.C. (1975).

[3] UNITED STATES NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, Rep. NUREG-1150, USNRC, Washington, DC (1990).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Advances in Reliability Analysis and Probabilistic Safety Assessment for Nuclear Power Reactors

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Legal and Governmental Infrastructure for Nuclear, Radiation, Radioactive Waste and Transport Safety, Safety Standards Series No. GS-R-1, IAEA, Vienna (2000).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Plants: Design, Safety Standard Series No. NS-R-1, IAEA, Vienna (2000).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification, draft Safety Guide, Vienna.

[8] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, Safety Series No. 75-INSAG-3, IAEA, Vienna (1988).

[9] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, The Format and Contents of Safety Analysis Reports for Nuclear Power Plants, draft Safety Guide IAEA, Vienna.

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Plants: Operation, Safety Standard Series No. NS-R-2, IAEA, Vienna (2000).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Safety Standards Series No. NS-G-2.2, IAEA, Vienna (2000).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Staffing, Recruitment, Qualification and Training of NPP Personnel, draft Safety Guide, IAEA, Vienna.

[14] UNITED STATED NUCLEAR REGULATORY COMMISSION, The Probabilistic Risk Assessment (PRA) Policy Statement (60 FR 42622), USNRC, Washington, DC (1995).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Living Probabilistic Safety Assessment (LPSA), IAEA-TECDOC-1106, Vienna (1999).

[16] FLEMING, K.N., Validation of PSAs for use in risk monitoring applications, ASME J. Pressure Vessel Technol. **120** (1998) 379–383.

[17] UNITED STATES NUCLEAR REGULATORY COMMISSION, Fault Tree Handbook, NUREG-0492, USNRC, Washington, D.C. (1981).

[18] UNITED STATES NUCLEAR REGULATORY COMMISSION, Probabilistic Risk Analysis: Procedures Guide, Rep. NUREG/CR-2300, USNRC, Washington, D.C. (1983).

[19] UNITED STATES NUCLEAR REGULATORY COMMISSION, Probabilistic Risk Analysis: Procedures Guide, Rev. 1, Reps NUREG/CR-2815 BNL-NUREG-51559, USNRC, Washington, D.C. (1985).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, The Role of Probabilistic Safety Assessments and Probabilistic Safety Criteria in Nuclear Power Plant Safety, Safety Series No. 106, IAEA, Vienna (1992).
[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Series No. 50-P-4, IAEA, Vienna (1992).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Safety Series No. 50-P-8, IAEA, Vienna (1995).
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), Safety Series No. 50-P-12, IAEA, Vienna (1996).
[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Reliability Analysis in Probabilistic Safety Assessments of Nuclear Power Plants, Safety Series No. 50-P-10, IAEA, Vienna (1995).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of External Hazards in Probabilistic Safety Assessments for Nuclear Power Plants, Safety Series No. 50-P-7, IAEA, Vienna (1995).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessments of Nuclear Power Plants for Low Power and Shutdown Modes, IAEA-TECDOC-1144, IAEA, Vienna (2000).
[27] UNITED STATES NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, Final Summary Report, Rep. NUREG/CR-1150, USNRC, Washington, D.C. (1990).
[28] UNITED STATES NUCLEAR REGULATORY COMMISSION, Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance, Rep. NUREG-1560, USNRC, Washington, D.C. (1997).
[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessment, Guidelines for the International Peer Review Service (IPERS) Programme, IAEA-TECDOC-832, 2nd edn, IAEA, Vienna (1995).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, A Framework for a Quality Assurance Programme for PSA, IAEA-TECDOC-1101, IAEA, Vienna (1999).
[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Review of Probabilistic Safety Assessments (PSA) Level 1, IAEA-TECDOC-1135, IAEA, Vienna (2000) (in co-operation with OECD/NEA).
[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Review of PSA Level 2, Draft IAEA-TECDOC (in co-operation with OECD/NEA).
[33] AMERICAN SOCIETY OF MECHANICAL ENGINEERS: Standard for Probabilistic Safety Assessment for Nuclear Power Plant Applications, New York, draft, ASME, New York.
[34] BOILING WATER REACTOR OWNER'S GROUP, Report to the Industry on PSA: Peer Review Certification Process: Pilot Plant Results, January 1997.
[35] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional Safety of Electrical/Electronic/Programmable Electronic safety related systems — Part 1: General Requirements, International Standard IEC 61508, IEC, Geneva (1998).
[36] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Risk analysis of technological systems, International Standard IEC 300-3-9, IEC, Geneva (1995).
[37] REINHARD, M., Presentation at CNRA Meeting, OECD/NEA, Paris, 29–30 November 1999.

[38] UNITED STATES NUCLEAR REGULATORY COMMISSION, An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant Specific Changes to the Licensing Basis, Regulatory Guide 1.174, USNRC, Washington, DC (1998).
[39] UNITED STATES NUCLEAR REGULATORY COMMISSION, Risk-Informed and Performance-Based Regulation, http://www.nrc.gov/NRC/COMMISSION/policy/whiteppr.html (2000)
[40] UNITED STATES NUCLEAR REGULATORY COMMISSION, New NRC Reactor Inspection and Oversight Program, Rep. NUREG-1649, Rev. 1, USNRC, Washington, DC (1999).
[41] UK HEALTH AND SAFETY EXECUTIVE, Health and Safety at Work Act (1974).
[42] UK HEALTH AND SAFETY EXECUTIVE, Nuclear Installations Act(1965).
[43] UK HEALTH AND SAFETY EXECUTIVE, The Tolerability of Risks from Nuclear Power Stations (1988).
[44] UK HEALTH AND SAFETY EXECUTIVE, Safety Assessment Principles for Nuclear Plants, HMSO, London (1992).
[45] UK HEALTH AND SAFETY EXECUTIVE, Reducing Risks, Protecting People, HSE Books, London (1999).
[46] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment, 75-INSAG-6, Vienna (1992).
[47] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments for Non-Reactor Nuclear Facilities , IAEA, Vienna (to be published).